Citation

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 150 506 A2 → A3 publ. 22.01.2003

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.10.2001 Bulletin 2001/44

(51) Int Cl.7: H04N 7/167, H04N 7/173, H04N 7/16

(21) Application number: 01660073.6

(22) Date of filing: 25.04.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 28.04.2000 US 559061

(71) Applicant: Nokia Corporation
02150 Espoo (FI)

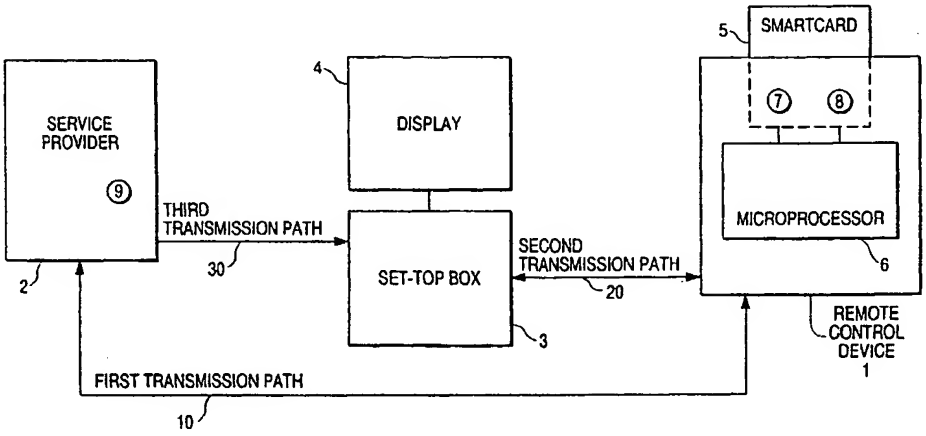
(72) Inventors:
- Ikonen, Ari M.
21280 Raisio (FI)
- Okkonen, Harri
Mountain View, CA 94041 (US)
- Heinonen, Pekka J.
02100 Espoo (FI)

(74) Representative: Johansson, Folke Anders et al
Nokia Corporation
P.O. Box 206
00045 Nokia Group (FI)

(54) **A method and system for providing secure subscriber content data**

(57) A personalized smart card stores therein public and private cryptography keys stored which are used to securely request and receive subscriber content data from a service provider, utilizing a remote control device.

FIG. 1



EP 1 150 506 A2

Description

Field of The Invention

[0001] The present invention relates to a system and method for providing a user with subscriber content data utilizing a remote control device which interacts with a service provider and set-top box over respective transmission paths. More specifically, the remote control device is smart card activated and enabled to provide a high level of security for the transmission of requests for subscriber content data and the transmission of the requested subscriber content data.

[0002] As advances are made in communications, especially wireless communications, and as efforts have been made to provide even more convenience for consumers, personal service providers have entered the homes and offices of their customers by providing their services by computer, television and other such multimedia terminals.

[0003] Examples of such services offered in the home include, but are certainly not limited to, personal banking, shopping and entertainment, which further includes pay-per-view programming and interactive video games.

[0004] To that end, European Patent Application EP 0 776 132 A2 describes an interactive television system in which service providers are able to provide services such as entertainment programs to users and also conduct electronic user polls, by utilizing terminals which communicate bidirectionally with a central computer. Each user of a terminal in the system is able to request services or even participate in polling by using a remote control apparatus. Furthermore, each remote control apparatus is registered to the respective user thereof, so that any message data issued by the respective remote control apparatus is accompanied by identifier information read out from a memory thereof for identifying the particular transmitting remote control apparatus. Individual user recognition by the remote control device can also be implemented using a plug-in IC card interface or fingerprint recognition section.

[0005] More particularly, though the remote control apparatus has a personal information storage section, with a remote control apparatus identifier stored therein to identify that specific remote control apparatus. Thus, before sending any message data from a user's assigned remote control apparatus, the user must first input a password in order to use the remote control apparatus.

[0006] Further, the remote control apparatus may include an encryption processing section by which the user's personal information can first be encrypted, and the encrypted code is then transmitted in place of the user's personal information in the transmitted data message.

[0007] Further still, in an effort to prohibit unauthorized users from using the specifically assigned remote control apparatus, the remote control apparatus may also include an interface section, or receptacle, for a plug-in IC (integrated circuit) card which enables the IC to be electrically connected via a data input port to a CPU (central processing unit). Thus, a user of the remote control apparatus must first insert the appropriate IC into the interface section, so that the CPU can execute processing to compare identification data stored on the IC with the user-specifying code stored in the remote control apparatus, to thereby effect recognition of the authorized user.

[0008] According to such embodiments, in order to request services through an interactive television system, a user thereof must therefore use a specifically assigned remote control apparatus which has user personal information stored therein in order to conduct interactive processing using a remote control apparatus.

[0009] Thus, existing security features of the interactive television system utilizing remote control apparatuses intended to prohibit non-designated users from using the specifically assigned remote control apparatus include (1) having a user enter a password to the remote control apparatus in order to activate the remote control apparatus, (2) attaching encrypted user-identification information to data messages transmitted from the remote control apparatus, and (3) comparing user identification information stored in the remote control apparatus with user identification information stored in a CPU by mounting an IC on the remote control apparatus which is connected to the CPU in order to perform the user identification information comparison.

[0010] However, the prior art is unable to ensure security of interactive transactions, including data requests and data transmissions between the user of a remote control apparatus and a service provider.

SUMMARY OF THE INVENTION

[0011] Therefore, it is an object of the present invention to provide an interactive multimedia personal service system in which a user utilizes a smart-card activated and enabled remote control device to interact with a service provider, via a set-top box, utilizing respective transmission paths, to securely request and receive subscriber content data.

[0012] According to a first aspect of the invention there is provided a method according to claim 1.

[0013] According to a second aspect of the invention there is provided a system according to claim 16.

[0014] According to a third aspect of the invention there is provided a method according to claim 2.

[0015] According to a fourth aspect of the invention there is provided a system according to claim 17.

[0016] The present invention relates to an interactive subscriber content data system which provides secure interaction between a user's remote control device, a set-top box and a service provider. An end user of the system holds a remote control device which may be a system-specific remote control device or a personal

hand-held device, a hand-held pager or a wireless telephone.

[0017] The remote control device provides secure transmissions for requests of subscriber content data since the remote control device is activated by the insertion of a user's personalized smart card into a reader which has contacts which contact corresponding contacts on a surface of the smart card. The smart card includes a security chip which includes personalized identification information for activating the remote control device, and further includes both a public key and a private key for encryption and decryption purposes, respectively.

[0018] After the user has activated the remote control device by inserting his or her personalized smart card into the reader, the user enters a request for subscriber content data using a key-pad or a smart touch pad on the remote control device. The request for subscriber content data as well as the user's public key, which is stored on the user's smart card, are then transmitted to the service provider over a first transmission path which is a two-way transmission path which includes a short message service (SMS).

[0019] In response to the request for subscriber content data from the user's remote control device, the following embodiments are provided, although the invention is not at all limited thereto.

[0020] According to an embodiment of the first and second aspect of the invention, the service provider receives the user's transmitted public key, encrypts a secret key corresponding to the service provider, and transmits the encrypted secret key corresponding to the service provider back to the remote control device, via the same two-way connection between the remote control device and the service provider on which the request for the subscriber content data was originally transmitted.

[0021] Upon receiving the encrypted secret key which has been encrypted using the user's public key from the service provider, the remote control device decrypts the service provider's secret key using the user's private key which is stored on the user's smart card. The remote control device then transmits the decrypted secret key corresponding to the service provider to a set-top box over a second transmission path which is a two-way connection between the remote control device and the set-top box. The two-way transmission path between the remote control device and the set-top box includes encrypted transmission connections such as a bluetooth connection.

[0022] The set-top box is a multi-media terminal which receives the requested subscriber content data from the service provider over a third transmission path. The third transmission path is a one-way broadcasting path from the service provider to the set-top box including a digital video broadcasting transmission (DVB-T). The requested content data is decrypted at the set-top box after the set-top box has received both the subscriber content data which has been encrypted by the service provider's secret key over the third transmission path and the decrypted secret key corresponding to the service provider from the remote control device over the second transmission path. Then the encrypted requested subscriber content data is decrypted and is then ready for display and/or further interactive activity ordered by the user of the remote control device.

[0023] According to an embodiment of the third and fourth aspect of the invention, after the request for subscriber content data and the user's public key have been transmitted from the user's remote control device to the service provider over the first transmission path, the service provider encrypts the secret key corresponding to the service provider using the user's transmitted public key and also encrypts the requested subscriber content data using the secret key. Then, the service provider transmits to the set-top box both the encrypted secret key corresponding to the service provider which has been encrypted using the user's public key and the requested subscriber content data which has been encrypted using the service provider's secret key. The transmission from the service provider to the set-top box is made over the third transmission path, which is the one-way transmission path from the service provider to the set-top box.

[0024] The set-top box then transmits the encrypted secret key to the remote control device over the second transmission path which includes the two-way encrypted connection between the set-top box and the remote control device. Upon receiving the encrypted secret key, the remote control device decrypts the service provider's secret key using the user's private key which is stored on the user's smart card. The remote control device then transmits the decrypted secret key corresponding to the service provider back to the set-top box over the second transmission path, thus enabling the encrypted subscriber content data to be decrypted at the set-top box using the service provider's secret key. The decrypted subscriber content data is then ready for display and/or further interactive activity ordered by the user of the remote control device.

[0025] It is noted that the transmission paths described above connecting the remote control device and the service provider, the remote control device and the set-top box, and the service provider and the set-top box, respectively, are the same for both embodiments described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] The scope of the present invention will be apparent from the following detailed description, when taken in conjunction with the accompanying drawings, and such detailed description, while indicating preferred embodiments of the invention, are given as illustrations only, since various changes and modifications within the spirit and scope of the invention will become apparent

to those skilled in the art from this detailed description, in which:

Fig. 1 shows a box-chart corresponding to a system embodiment of the present invention;
Fig. 2 shows a flowchart of the processing according to a first method embodiment of the present invention; and
Fig. 3 shows a flowchart of the processing according to a second method embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0027] In the detailed description of the subject invention which follows, when appropriate, like reference numerals and characters may be used to designate identical, corresponding or similar components in different figure drawings. Furthermore, example sizes/models/values/ranges may be given, although the present invention is not intended to be so limited.

[0028] According to an example embodiment of the present invention, an interactive subscriber content data system provides secure interaction between a user's remote control device, a set-top box and a service provider. As shown in Fig. 1, for example, an end user of the system holds a remote control device 1 which may be a system-specific remote control device or a personal hand-held device including, but not limited to, a hand-held pager or a wireless telephone.

[0029] The remote control device 1 provides secure transmissions for requests of subscriber content data since the remote control device 1 is activated by the insertion of a user's personalized smart card 5 into the remote control device 1 where it is read. The smart card 5 includes a security chip which includes personalized identification information for activating the remote control device, and further includes both a public key 7 and a private key 8 for encryption and decryption purposes, respectively.

[0030] Figs. 2 and 3, described below, represent two example method embodiments of the present invention for securely requesting and receiving subscriber content data utilizing the system of Fig. 1 described above, although the present invention is not limited only to such descriptions.

[0031] The method embodiments described in both Figs. 2 and 3 start with step 100 whereby a user has activated a remote control device by reading the user's personalized smart card 5. The subsequent steps of the method embodiment of Fig. 2 will be described next. In step 200, the user enters a request for subscriber content data using a key-pad or a smart touch pad on the remote control device 1. The request for subscriber content data as well as the user's public key 7, which is stored on the user's smart card 5, are then both transmitted to the service provider 2 over a first transmission path 10 which is a two-way transmission path which includes, but is not limited to, a short message service (SMS). The first transmission path may be in accordance with diverse types of transmission mechanisms including, but not limited to, GSM, CDMA, UMTS, etc. SMS is a type of pager service within the Global System for Mobile Communications (GSM) mobile phone system that supports messages up to 160 characters in length. SMS supports binary formats, and messages ride on a separate signaling path so they are transmitted simultaneously with voice, data and fax. GSM is a digital cellular phone technology based on Time Division Multiple Access system (TDMA) that is widely deployed in Europe and throughout the world, operating in the 1.8 to 1.9 GHz band, compared to 800-900MHz for other cellular systems. TDMA is a satellite and cellular phone technology that interleaves multiple digital signals onto a single high-speed channel.

[0032] The service provider 2 receives the user's transmitted public key, and, in step 200, encrypts a secret key 9 corresponding to the service provider and transmits the encrypted secret key 9 corresponding to the service provider back to the remote control device, via the same two-way connection between the remote control device and the service provider on which the request for the subscriber content data was originally transmitted. Step 200 may also include the encryption of the requested subscriber content data by the service provider using the user's transmitted public key 7, and the further transmission of the encrypted requested content data to the set-top box 3 from the service provider 2.

[0033] Upon receiving the encrypted secret key 9 which has been encrypted using the user's public key from the service provider, in step 210 the remote control device decrypts the service provider's secret key 9 using the user's private key 8 which is stored on the user's smart card 5. In step 220, the remote control device 1 then transmits the decrypted secret key 9 corresponding to the service provider to a set-top box 3 over a second transmission path 20 which is a two-way connection between the remote control device 1 and the set-top box 3. The two-way transmission path 20 between the remote control device 1 and the set-top box 3 includes, but is not limited to, encrypted transmission connections such as a bluetooth connection. Bluetooth protocol is a radio frequency protocol having a radio frequency range of 100m to 1000m.

[0034] Furthermore, the set-top box 3 is a multi-media terminal which receives, in step 200, the encrypted requested subscriber content data from the service provider over a third transmission path 30. The third transmission path 30 is a one-way broadcasting path from the service provider to the set-top box including, but not limited to, a digital video broadcasting transmission (DVB-T). DVB is an international digital broadcast standard for TV, audio and data which can be broadcast via satellite, cable or terrestrial systems.

[0035] If the first transmission path 10 is not available

for any reason, as an alternative when the remote controller is used, a fourth path (not illustrated), which performs the function of the first path, may be used which is comprised of the second path 20 and a telephone modem connection between the set top box 3 and the service provider 2. The set-top box 3 may include a wireless modem.

[0036] The encrypted requested content data is decrypted at the set-top box 3 after the set-top box 3 has received both the subscriber content data which has been encrypted by the service provider's secret key 9 over the third transmission path 30 (step 200) and the decrypted secret key 9 corresponding to the service provider from the remote control device 1 over the second transmission path 20 (step 220). Then in step 230 the encrypted requested subscriber content data is decrypted using the service provider's secret key 9 and is then ready for display and/or further interactive activity ordered by the user of the remote control device, as shown by step 240.

[0037] In a second method embodiment of the present invention, as shown in Fig. 3, after the step 100 request for subscriber content data and the user's public key 7 have been transmitted from the user's remote control device 1 to the service provider 2 over the first transmission path 10, in step 300 the service provider 2 transmits to the set-top box 3 the secret key 9 corresponding to the service provider 2 which is encrypted using the user's transmitted public key 7 and the requested subscriber content data which is encrypted using the secret key 9. The service provider 2 transmits the encrypted secret key 9 and the encrypted requested subscriber content data over one-way third transmission path 300, which is described above.

[0038] In step 310, the set-top box 3 then transmits the encrypted secret key 9 to the remote control device 1 over the second transmission path 20. Upon receiving the encrypted secret key 9, in step 320 the remote control device 1 decrypts the service provider's secret key 9 using the user's private key 8 which is stored on the user's smart card 5. It should be noted that for all method embodiments, including but not limited to those shown in Figs. 2 and 3, the smart card 5 may either remain inserted in the remote control device 1 or the smart card 5 may be read by the remote control device 1 with the personal information of the user, including the user's public key 7 and private key 8 being downloaded onto the process 6 of the remote control device 1.

[0039] In step 330, the remote control device 1 transmits the decrypted secret key 9 corresponding to the service provider 2 back to the set-top box 3 over the second transmission path 20, thus enabling step 340 whereby the encrypted subscriber content data to be decrypted at the set-top box 3 using the service provider's secret key 9. The decrypted subscriber content data is then ready for display and/or further interactive activity ordered by the user of the remote control device, as shown by step 350.

[0040] Thus, the present invention in a preferred embodiment utilizes cryptography keys stored in personalized smart cards in combination with cryptography keys corresponding to respective service providers, to enable a user to use a remote control device to securely request subscriber content data from a service provider and securely receive the requested subscriber content data from the service provider.

[0041] While the present invention has been described in detail and pictorially in the accompanying drawings, it is not limited to such details since many changes and modifications may be made thereto without departing from the scope of the present claims. For example, the transfer of keys over the second transmission path 20 could be eliminated if the content data is encrypted or decrypted on the smart card. It is intended that all such modifications fall within the scope of the following claims.

Claims

1. A method for providing content data from a service provider to a requesting end user, said method comprising the steps of:

   transmitting, through a first transmission path, from a remote control device corresponding to said end user to a service provider, a public key and a request for content data;
   transmitting, through said first transmission path, a secret key encrypted by said public key from said service provider to said remote control device;
   receiving said secret key encrypted by said public key from said service provider at said remote control device;
   decrypting, at said remote control device, the secret key using a private key corresponding to said public key of said end user;
   transmitting, through a second transmission path, from said remote control device to a set-top box, the decrypted secret key corresponding to said service provider;
   transmitting, through a third transmission path, from said service provider to said set-top box, the requested content data encrypted by said secret key; and
   decrypting the encrypted content data, by said set-top box, using the secret key corresponding to said service provider.

2. A method for providing content data from a service provider to a requesting end user, said method comprising the steps of:

   transmitting, through a first transmission path, from a remote control device to a service pro-

vider, a public key and a request for content data;
transmitting, through a third transmission path, from said service provider to a set-top box, a secret key corresponding to said service provider encrypted by said public key and the requested content data encrypted by said secret key;
transmitting, through a second transmission path, from said set-top box to said remote control device, the encrypted secret key corresponding to said service provider;
decrypting, by said remote control device, said secret key corresponding to said service provider using a private key corresponding to said public key of said end user;
transmitting, through said second transmission path, from said remote control device to said set-top box, the decrypted secret key corresponding to said service provider; and
decrypting, by said set-top box, the encrypted content data using the secret key corresponding to said service provider.

3. A method according to Claim 1 or 2, wherein said first transmission path is a two-way data or messaging connection between said remote control device and said service provider.

4. A method according to Claim 3, wherein said two-way TDMA connection is a two-way GSM (Global System for Mobile Communications) connection between said remote control device and said service provider.

5. A method according to Claim 4, wherein said two-way GSM connection is a two-way SMS (Short Message Service) connection between said remote control device and said service provider.

6. A method according to Claim 1 or 2, wherein said second transmission path is encrypted.

7. A method according to Claim 6, wherein said second transmission path is a two-way bluetooth connection between said remote control device and said set-top box.

8. A method according to Claim 1 or 2, wherein said third transmission path is a one-way transmission path from said service provider to said set-top box.

9. A method according to Claim 8, wherein said one-way transmission path is a DVB (Digital Video Broadcasting) transmission path.

10. A method according to Claim 1 or 2, wherein said remote control device is activated by a smart card, and said smart card stores said public key and said private key corresponding to said end user.

11. A method according to Claim 1 or 2, wherein said set-top box is a multi-media terminal.

12. A method according to Claim 11, wherein said multi-media terminal is an electronic notebook.

13. A method according to Claim 11, wherein said multi-media terminal is a television set.

14. A method according to Claim 1 or 2, wherein said remote control device is a hand-held pager.

15. A method according to Claim 1 or 2, wherein said remote control device is a telephone.

16. A subscriber data content service receiving system, comprising:

a remote control device corresponding to an end user;
a set-top box; and
a service provider;
wherein:

said remote control device is configured to transmit to a service provider, through a first transmission path, a public key and a request for content data;
said service provider is configured to transmit to said remote control device, through said first transmission path, a secret key encrypted by said public key;
said remote control device is configured to receive said secret key encrypted by said public key from said service provider;
said remote control device is configured to decrypt said secret key using a private key corresponding to said public key of said end user;
said remote control device is configured to transmit to said set-top box, through a second transmission path, the decrypted secret key corresponding to said service provider;
said service provider is configured to transmit to said set-top box, through a third transmission path, the requested content data encrypted by said secret key; and
said set-top box is configured to decrypt the encrypted content data using the secret key corresponding to said service provider.

17. A subscriber data content service receiving system, comprising:

a remote control device corresponding to an end user;
a set-top box; and
a service provider;
wherein:

said remote control device is configured to transmit to a service provider, through a first transmission path, a public key and a request for content data;
said service provider is configured to transmit to a set-top box, through a third transmission path, a secret key corresponding to said service provider encrypted by said public key and the requested content data encrypted by said secret key;
said set-top box is configured to transmit to said remote control device, through a second transmission path, the encrypted secret key;
said remote control device is configured to decrypt said secret key corresponding to said service provider using a private key corresponding to said public key of said end user;
said remote control device is configured to transmit to said set-top box, through said second transmission path, the decrypted secret key corresponding to said service provider; and
said set-top box is configured to decrypt the encrypted content data using the secret key corresponding to said service provider.

18. A system according to Claim 16 or 17, wherein said first transmission path is a two-way TDMA connection between said remote control device and said service provider.

19. A system according to Claim 18, wherein said TDMA connection is a two-way GSM (Global System for Mobile Communications) connection between said remote control device and said service provider.

20. A system according to Claim 19, wherein said GSM connection is a two-way SMS (Short Message Service) connection between said remote control device and said service provider.

21. A system according to Claim 16 or 17, wherein said second transmission path is encrypted.

22. A system according to Claim 21, wherein said second transmission path is a two-way bluetooth connection between said remote control device and said set-top box.

23. A system according to Claim 16 or 17, wherein said third transmission path is a one-way transmission path from said service provider to said set-top box.

24. A system according to Claim 23, wherein said one-way transmission path is a DVB (Digital Video Broadcasting) transmission path.

25. A system according to Claim 16 or 17, wherein said remote control device is configured to be activated by a smart card, and said smart card is configured to store said public key and said private key corresponding to said end user.

26. A system according to Claim 16 or 17, wherein said set-top box is a multi-media terminal.

27. A system according to Claim 26, wherein said multimedia terminal is an electronic notebook.

28. A system according to Claim 26, wherein said multimedia terminal is a television set.

29. A system according to Claim 16 or 17, wherein said remote control device is a hand-held pager.

30. A system according to Claim 16 or 17, wherein said remote control device is a telephone.

FIG. 1

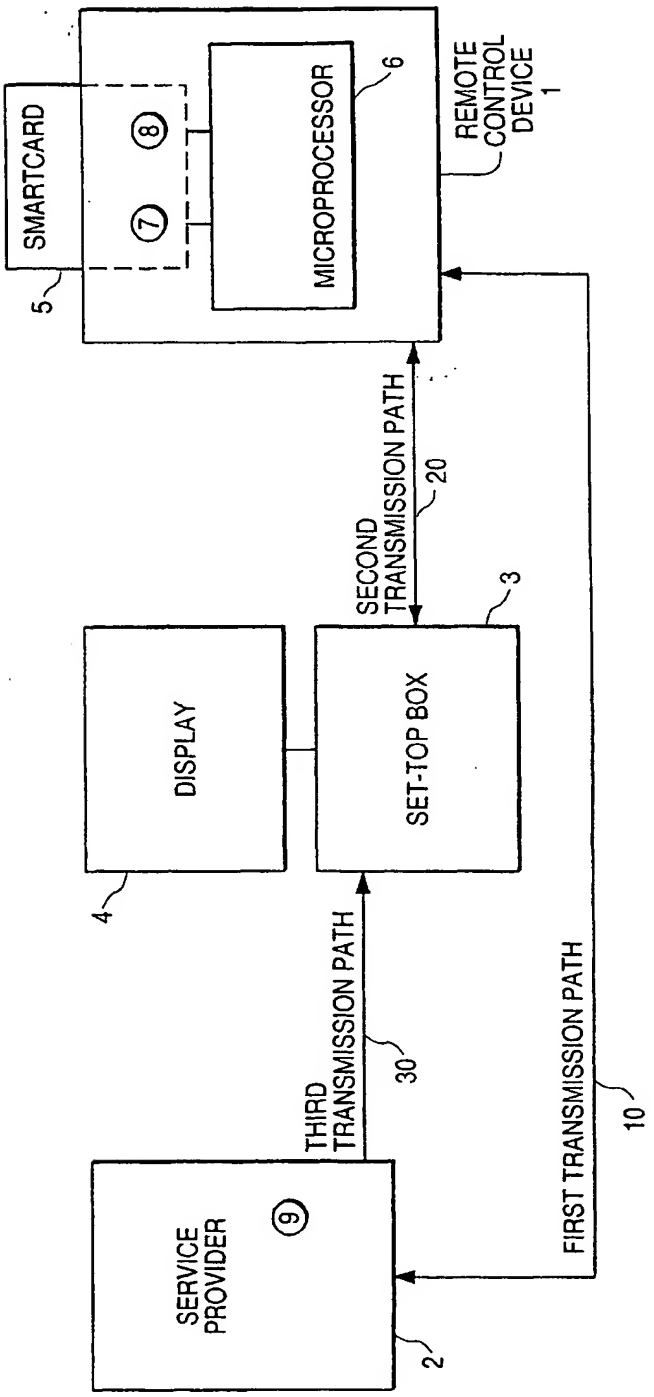

SMARTCARD
8
7
MICROPROCESSOR
6
REMOTE CONTROL DEVICE
1
5
SECOND TRANSMISSION PATH
20
3
DISPLAY
SET-TOP BOX
4
THIRD TRANSMISSION PATH
30
FIRST TRANSMISSION PATH
10
SERVICE PROVIDER
9
2

FIG. 2

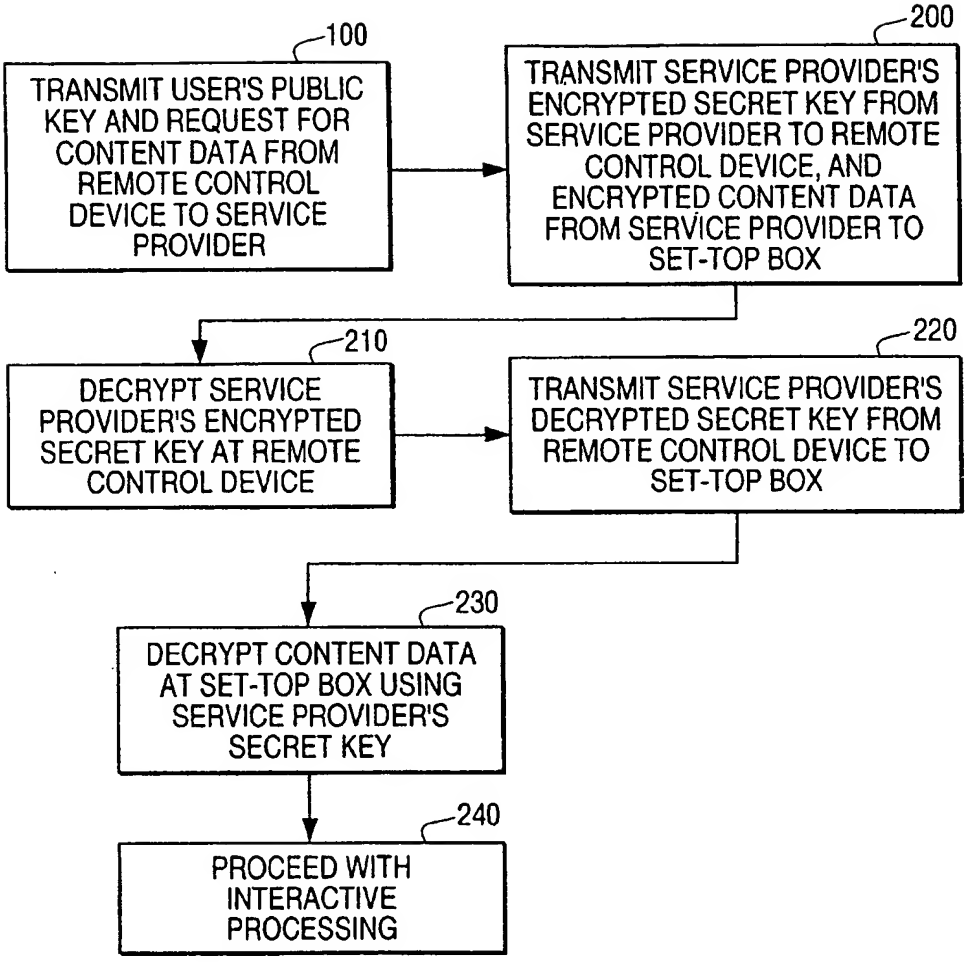
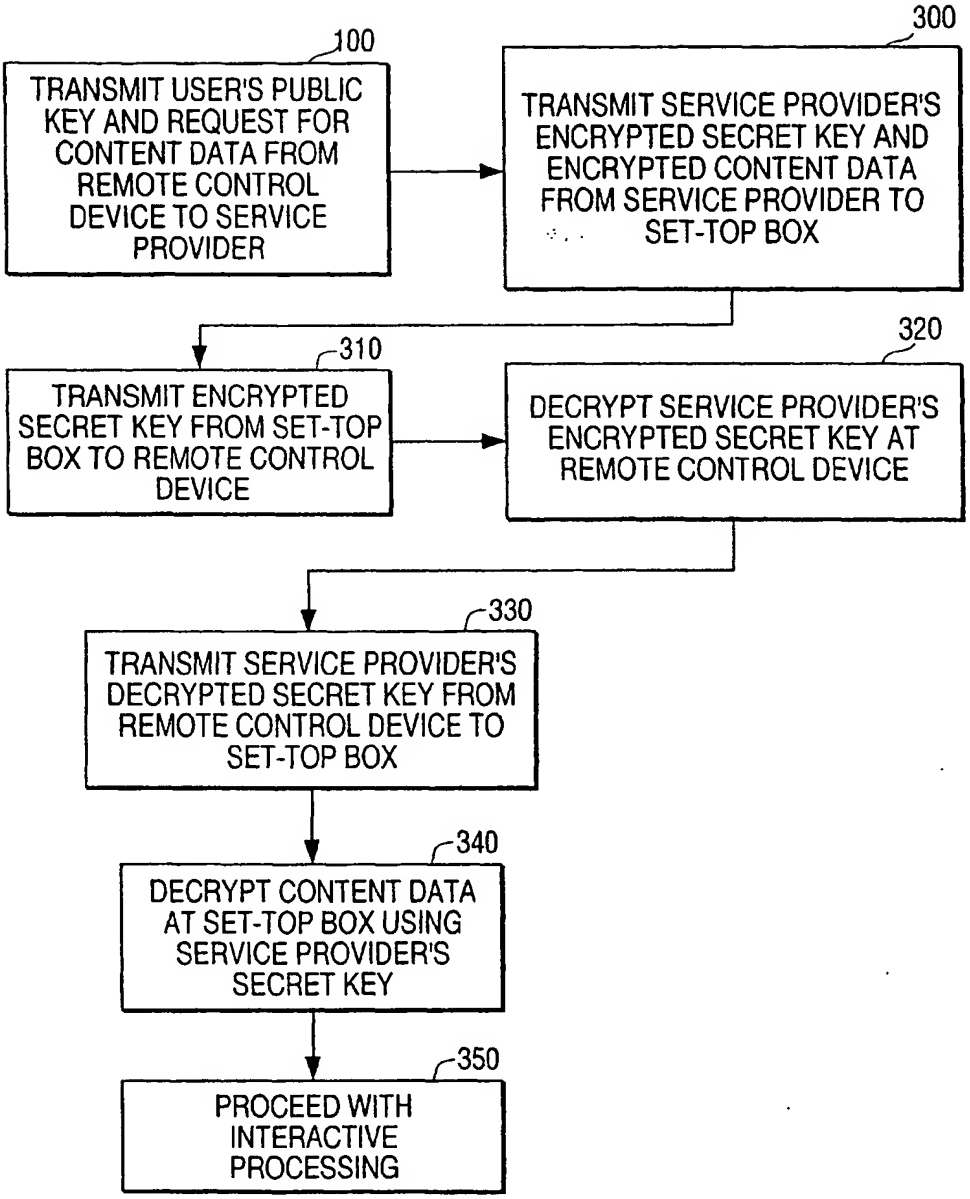

100
TRANSMIT USER'S PUBLIC KEY AND REQUEST FOR CONTENT DATA FROM REMOTE CONTROL DEVICE TO SERVICE PROVIDER
200
TRANSMIT SERVICE PROVIDER'S ENCRYPTED SECRET KEY FROM SERVICE PROVIDER TO REMOTE CONTROL DEVICE, AND ENCRYPTED CONTENT DATA FROM SERVICE PROVIDER TO SET-TOP BOX
210
DECRYPT SERVICE PROVIDER'S ENCRYPTED SECRET KEY AT REMOTE CONTROL DEVICE
220
TRANSMIT SERVICE PROVIDER'S DECRYPTED SECRET KEY FROM REMOTE CONTROL DEVICE TO SET-TOP BOX
230
DECRYPT CONTENT DATA AT SET-TOP BOX USING SERVICE PROVIDER'S SECRET KEY
240
PROCEED WITH INTERACTIVE PROCESSING

FIG. 3


100
TRANSMIT USER'S PUBLIC KEY AND REQUEST FOR CONTENT DATA FROM REMOTE CONTROL DEVICE TO SERVICE PROVIDER
300
TRANSMIT SERVICE PROVIDER'S ENCRYPTED SECRET KEY AND ENCRYPTED CONTENT DATA FROM SERVICE PROVIDER TO SET-TOP BOX
310
TRANSMIT ENCRYPTED SECRET KEY FROM SET-TOP BOX TO REMOTE CONTROL DEVICE
320
DECRYPT SERVICE PROVIDER'S ENCRYPTED SECRET KEY AT REMOTE CONTROL DEVICE
330
TRANSMIT SERVICE PROVIDER'S DECRYPTED SECRET KEY FROM REMOTE CONTROL DEVICE TO SET-TOP BOX
340
DECRYPT CONTENT DATA AT SET-TOP BOX USING SERVICE PROVIDER'S SECRET KEY
350
PROCEED WITH INTERACTIVE PROCESSING